

Oracle Access Manager Integration
Oracle FLEXCUBE Universal Banking
Release 12.1.0.0.0
September 2019



Table of Contents

1. PREFACE	1-3
1.1 INTRODUCTION	1-3
1.2 AUDIENCE	1-3
1.3 ABBREVIATIONS	1-3
1.4 DOCUMENTATION ACCESSIBILITY	1-3
1.5 ORGANIZATION	1-3
1.6 GLOSSARY OF ICONS	1-4
1.6.1 <i>Related Documents</i>	1-4
2. ENABLING SINGLE SIGN-ON WITH ORACLE ACCESS MANAGER	2-1
2.1 INTRODUCTION	2-1
2.2 BACKGROUND AND PREREQUISITES	2-1
2.2.1 <i>Software Requirements</i>	2-1
2.3 BACKGROUND OF SSO RELATED COMPONENTS	2-2
2.3.1 <i>Oracle Access Manager (OAM)</i>	2-2
2.3.2 <i>LDAP Directory Server</i>	2-2
2.3.3 <i>WebGate/AccessGate</i>	2-2
2.3.4 <i>Oracle Adaptive Access Manager</i>	2-3
2.4 ASSUMPTIONS	2-3
2.5 INSTALL AND CONFIGURE ORACLE ACCESS MANAGER	2-3
2.5.1 <i>Installation of Infrastructure and OAM</i>	2-3
2.5.2 <i>Run the Repository Creation Utility</i>	2-3
2.5.3 <i>Configure the Oracle Access Management 12c Domain</i>	2-4
2.5.4 <i>Start the Servers</i>	2-6
2.6 INSTALL AND CONFIGURE ORACLE UNIFIED DIRECTORY	2-7
2.6.1 <i>Install Oracle Unified Directory</i>	2-7
2.6.2 <i>Configure Oracle Unified Directory</i>	2-7
2.6.3 <i>Configure OUD as the Identity Store in OAM</i>	2-8
2.7 INSTALL AND CONFIGURE ORACLE HTTP SERVER 12C	2-10
2.7.1 <i>Install Oracle HTTP Server</i>	2-10
2.7.2 <i>Configure HTTP Server</i>	2-11
2.7.3 <i>Start the Servers</i>	2-12
2.8 CREATING OAM 12C WEBGATE	2-12
2.8.1 <i>Post OAM Webgate 12c Creation</i>	2-17

1. Preface

1.1 Introduction

This manual discusses the integration of Oracle FLEXCUBE Universal Banking and the Oracle Access Manager system. The configurations required for proper functioning of this integration and further processing are documented in this manual.

1.2 Audience

This manual is intended for the following User/User Roles:

Role	Function
Back office data entry Clerks	Input functions for maintenance related to the interface.
Implementation team	Implementation of Oracle FLEXCUBE Investor Servicing

1.3 Abbreviations

Abbreviation	Description
System	Unless specified, it shall always refer to Oracle FLEXCUBE
OAM	Oracle Access Manager
OHS	Oracle HTTP Server
ODU	Oracle Unified Directory
UBS	Universal Banking Solutions
SSO	Single Sign-on
LDAP	Lightweight Directory Access Protocol

1.4 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.





1.5 Organization

This manual is organized into the following chapters:

Chapter 1	<i>Preface</i> gives information on the intended audience. It also lists the various chapters covered in this User Manual.
Chapter 2	<i>Enabling Single Sign-on (SSO) with Oracle Access Manager</i> discusses the method to integrate Oracle FLEXCUBE with Oracle Access Manager for Single Sign-on.

1.6 **Glossary of Icons**

This User Manual may refer to all or some of the following icons.

Icons	Function
	Exit
	Add row
	Delete row
	Option List

1.6.1 **Related Documents**

You may refer the following manual for more information

- Oracle Access Manager User Manual (not included with Oracle FLEXCUBE User Manuals)

2. Enabling Single Sign-on with Oracle Access Manager

2.1 Introduction

For the purpose of single sign-on FLEXCUBE is qualified with Oracle Identity Management 12.2.1.3.0 (Fusion Middleware 12cR2) – specifically using the Access Manager component of Oracle Identity Management. This feature is available in FLEXCUBE since the release FC UBS V.UM 7.3.0.0.0.0 .

This document provides an understanding as to how single sign-on can be enabled for a FLEXCUBE deployment using Oracle Fusion Middleware 12cR2.

In addition to providing a background to the various components of the deployment, this document also talks about Configuration to be done in FLEXCUBE and Oracle Access Manager to enable single sign-on using Oracle Internet Directory as a LDAP server.

2.2 Background and Prerequisites

2.2.1 Software Requirements

Oracle Identity and Access Management 12c R2 - 12.2.1.3.0

- JDK 1.8 for Linux x64
- Oracle Middleware (WLS) (12.2.1.3.0) software
- Oracle Access Manager – 12.2.1.3.0
- Oracle Unified Directory - 12.2.1.3.0
- Oracle Fusion Middleware Web Tier Utilities 12c - 12.2.1.3.0
 - Oracle HTTP Server
- Optional: Oracle Adaptive Access Manager – 12.2.1.3.0 (Strong Authentication purpose only)

LDAP Directory Server

Please make sure that the LDAP server to be used for FLEXCUBE Single Sign on deployment is certified to work with OAM.

List of few LDAP Directory servers supported as per OAM document (note – this is an indicative list. The conclusive list can be obtained from the Oracle Access Manager documentation. Though we have only use OUD for our testing purposes):

- Oracle Unified Directory
- Active Directory
- ADAM
- ADSI
- Data Anywhere (Oracle Virtual Directory)
- IBM Directory Server
- NDS
- Sun Directory Server
- Oracle Weblogic

For the purpose of achieving single sign on for FLEXCUBE in FMW 12cR2, it is necessary for the weblogic instance to have an explicit **Oracle HTTP server (OHS)**.

2.3 Background of SSO related components

2.3.1 Oracle Access Manager (OAM)

Oracle Access Manager consists of the Access System and the Identity System. The Access System secures applications by providing centralized authentication, authorization and auditing to enable single sign-on and secure access control across enterprise resources. The Identity System manages information about individuals, groups and organizations. It enables delegated administration of users, as well as self-registration interfaces with approval workflows. These systems integrate seamlessly.

The backend repository for the Access Manager is an LDAP-based directory service that can be a combination of a multiple directory servers, which is leveraged for two main purposes:

- As the store for policy, configuration and workflow related data, which is used and managed by the Access and Identity Systems
- As the identity store, containing the user, group and organization data that is managed through the Identity System and is used by the Access System to evaluate access policies.

2.3.2 LDAP Directory Server

To integrate Flexcube with OAM to achieve Single Sign-on feature, Flexcube's password policy management, like password syntax and password expiry parameters will no longer be handled by Flexcube. Instead, the password policy management can be delegated to the Directory Server. All password policy enforcements would be on the LDAP user id's password and NOT Flexcube application users' passwords.

2.3.3 WebGate/AccessGate

A WebGate is a Web server plug-in that is shipped out-of-the-box with Oracle Access Manager. The WebGate intercepts HTTP requests from users for Web resources and forwards it to the Access Server for authentication and authorization.

Whether you need a WebGate or an AccessGate depends on your use of the Oracle Access Manager Authentication provider. For instance, the:

Identity Asserter for Single Sign-On: Requires a separate WebGate and configuration profile for each application to define perimeter authentication. Ensure that the Access Management Service is On.

Authenticator or Oracle Web Services Manager: Requires a separate AccessGate and configuration profile for each application. Ensure that the Access Management Service is On.

2.3.4 Oracle Adaptive Access Manager

Oracle Adaptive Access Manager provides an innovative, comprehensive feature set to help organizations prevent fraud and misuse. Strengthening standard authentication mechanisms, innovative risk-based challenge methods, intuitive policy administration and integration across the Identity and Access Management Suite and with third party products make Oracle Adaptive Access Manager uniquely flexible and effective. Oracle Adaptive Access Manager provides real-time and batch risk analytics to combat fraud and misuse across multiple channels of access. Real-time evaluation of multiple data types helps stop fraud as it occurs. Oracle Adaptive Access Manager makes exposing sensitive data, transactions and business processes to consumers, remote employees or partners via your intranet and extranet safer.

Oracle Adaptive Access Manager provides an extensive set of capabilities including device fingerprinting, real-time behavioral profiling and risk analytics that can be harnessed across both Web and mobile channels. It also provides risk-based authentication methods including knowledge-based authentication (KBA) challenge infrastructure with Answer Logic and OTP Anywhere server-generated one-time passwords, delivered out of band via Short Message Service (SMS), e-mail or Instant Messaging (IM) delivery channels. Oracle Adaptive Access Manager also provides standard integration with Oracle Identity Management, the industry leading identity management and Web Single Sign-On products, which are integrated with leading enterprise applications.

2.4 Assumptions

- The steps provided below assume that FLEXCUBE has already been deployed and is working (without single sign-on)
- For simplicity, the Steps followed in the document used non-ssl configuration. For production environment it is recommended to use SSL configuration.

2.5 Install and Configure Oracle Access Manager

2.5.1 Installation of Infrastructure and OAM

1. Run the following command to install WebLogic Server and complete all the steps:

```
cd /stage
unzip fmw_12.2.1.3.0_infrastructure_Disk1_1of1.zip
java -jar /stage/fmw_12.2.1.3.0_infrastructure.jar
```

Installation Type	Colocated Oracle Identity and Access Management (Managed through WebLogic Server)
-------------------	--

2. After the above installation, install OAM binary in the above installed directory.

```
java -jar /stage/fmw_12.2.1.3.0_idm.jar
```

2.5.2 Run the Repository Creation Utility

1. Launch a terminal window and enter the following command

```
cd /u01/app/oracle/product/middleware/oracle_common/bin
./rcu
```

2. Follow the table below to guide you through the installation screens:

Step	Window Description	Choices or Values
1.	Welcome1	Click Next
2.	Create Repository	System Load and Product Load
3.	Database Connection Details	Database Type: Oracle Database Host Name: oam.example.com Port: 1521 Service Name: orcl.example.com Username: sys Password: Welcome1 Role: SYSDBA Click OK in Checking Prerequisites window
4.	Checking Prerequisites	Click OK
5.	Select Components	Create a new prefix: DEV Select schema: Oracle Access Manager Click OK in Checking Prerequisites window
6.	Schema Passwords	Use same passwords for all schemas Password: Welcome1 Confirm Password: Welcome1
7.	Map Tablespaces	Click Next Click OK in Confirmation and Creating Tablespaces window
8.	Summary	Click Create
9.	Completion Summary	Click Close

2.5.3 Configure the Oracle Access Management 12c Domain

1. Launch a terminal window and enter the following command if RCU database is in RAC else follow step 2.
cd /u01/app/oracle/product/middleware/oracle_common/common/bin
./config.sh

2. If RCU database is not RAC then follow this step. Edit config_internal.sh in /u01/app/oracle/product/middleware/oracle_common/common/ and add -Doracl e.j dbc. fanEnabl ed=fal se in JVM_ARGS and save the file.

Exampl e:

```
JVM_ARGS="-Dpython.cachedir=/tmp/cachedir -Doracl e.j dbc. fanEnabl ed=fal se
${JVM_D64} ${JVM_D64} ${UTILS_MEM_ARGS} ${SECURITY_JVM_ARGS}
${CONFIG_JVM_ARGS}"
```

Launch ./config.sh

3. Follow the table below to guide you through the configuration screens:

Step	Window Description	Choices or Values
1.	Create Domain	Select Create a new domain Domain Location: /u01/app/oracle/admin/domains/oam_domain
2.	Templates	Create Domain Using Product Templates Select: Oracle Access Management Suite
3.	Application Location	Application Location: /u01/app/oracle/admin/applications/oam_domain
4.	Administrator Account	Name: weblogic Password: Welcome1 Confirm: Welcome1
5.	Domain Mode and JDK	Domain Mode: Production JDK: Oracle Hotspot
6.	Database Configuration Type	Host Name: oam.example.com DMS/Service: orcl.example.com Port: 1521 Schema Owner: DEV_STB Schema Password: Welcome1 Click Get RCU Configuration If successful click Next
7.	Component Datasources	Click Next
8.	JDBC Component Schema Test	Click Next

9.	Advanced Configuration	Select Node Manager , and Topology
10.	Node Manager	Node Manager Type: Per Domain Default Location Username: weblogic Password: Welcome1 Confirm Password: Welcome1
11.	Managed Servers	Click Next
12.	Clusters	Click Next
13.	Server Templates	Click Next
14.	Coherence Clusters	Click Next
15.	Machines	Click Add Name: oam_machine
16.	Assign Servers to Machines	Select Admin Server , oam_server1 and oam_policy_mgr1 . Select oam_machine and click the right arrow to move the servers under oam_machine
17.	Virtual Targets	Click Next
18.	Partitions	Click Next
19.	Configuration Summary	Click Create
20.	Configuration Progress	Click Next
21.	End of Configuration	Click Finish

2.5.4 Start the Servers

1. Launch a terminal window as `oracle` and enter the following commands to start the Oracle Access Management 12c AdminServer
`cd /u01/app/oracle/admin/domains/oam_domain/
./startWebLogic.sh`
2. In another terminal window start Node Manager by running the following command:
`nohup ./startNodeManager.sh`
3. Test the installation

Start a browser and access the Oracle Access Management Console at `http://oam.example.com:7001/oamconsole`. Login as `weblogic/Welcome1`.

Access <http://oam.example.com:14150/access> and login with weblogic/Welcome1.

2.6 Install and Configure Oracle Unified Directory

2.6.1 Install Oracle Unified Directory

1. Launch a terminal window and enter the following command:
`java -jar fmw_12.2.1.3.0_oud_generic.jar`
2. Follow the table below to guide you through the installation screens. For internal testing purpose we have used Standalone Installation and uploaded some sample user data.

Step	Window Description	Choices or Values
1.	Welcome	Click Next
2.	Auto Updates	Skip Auto Updates
3.	Installation Location	Oracle Home: /u01/app/oracle/product/middleware/oud
4.	Installation Type	Standalone Oracle Unified Directory Server (Managed independently of WebLogic Server)
5.	Prerequisite Checks	Click Next
6.	Installation Summary	Click Install
7.	Installation Progress	Click Next
8.	Installation Complete	Click Finish

2.6.2 Configure Oracle Unified Directory

1. Launch a terminal window as `oracle` and enter the following command:

```
2. cd /u01/app/oracle/product/middleware/oud/oud
```

```
./oud-setup
```

3. Follow the table below to guide you through the configuration screens:

Step	Window Description	Choices or Values
1.	Welcome	Click Next
2.	Server Administration Settings	Instance Path: /u01/app/oracle/product/middleware/oud/asinst_1/OUT Host Name: oam.example.com Password: Welcome1 Confirm Password: Welcome1
3.	Ports	Select Checkbox: LDAPS: Enable on Port
4.	Topology Options	Select: This will be a standalone server
5.	Directory Data	Select: Leave Database Empty
6.	Oracle Components Integration	Click Next
7.	Server Tuning	Click Next
8.	Review	Click Finish
9.	Finished	Click Close

4. Import sample identity data(empl.ldif) including some users and groups. Run the following command to populate the oud1 directory server with sample data:

```
cd /u01/app/oracle/product/middleware/oud/asinst_1/OUT/bin
```

```
./ldapmodify -p 1389 -D "cn=Directory Manager" -w Welcome1 -a -c -f /stage/example.ldif
```

2.6.3 Configure OUD as the Identity Store in OAM

1. Launch a browser and login to the OAM Console (<http://oam.example.com:7001/oamconsole>) as weblogic/Welcome1.

2. Click the Configuration tab (top right), then click User Identity Stores. Click Create in the OAM ID Stores section.
3. Specify the values as shown:
 - o **Store Name:** OUD Store
 - o **Store Type:** OUD: Oracle Unified Directory
 - o **Location:** oam.example.com:1389
 - o **Bind DN:** cn=Directory Manager
 - o **Password:** Welcome1
 - o **Login ID Attribute:** uid
 - o **User Password Attribute :** userPassword
 - o **User Search Base:** ou=People,dc=example,dc=com
 - o **Group Name Attribute:** cn
 - o **Group Search Base:** ou=Groups, dc=example, dc=com
4. Click **Test Connection**. Assuming the connection works, click **OK** in the Connection Status window.
5. Click **Apply** to save the definition.
6. Access the **User Identity Stores** tab, and set **Default Store** to OUD_Store, and then Click **Apply**.
7. Click **Application Security**, and then **Authentication Modules** under the **Plug-ins** tile.
8. Click **Create > Create LDAP Authentication Module**. Enter the following values and click **Apply**:
 - o **Name:** LDAPOverOUD
 - o **User Identity Store:** OUD_Store
9. Click the **Launch Pad** tab, and click the **Authentication Schemes** link in the Access Manger tile. In the **Search Authentication Schemes** page, click **Search**. Select the **LDAPScheme** row in the search result and click **Edit**.
In the **LDAPScheme**, click **Duplicate**. It creates a new scheme with the name '**Copy of LDAP Scheme**'. Change this scheme as follows, and then click **Apply**.

Basic Style Authentication Scheme

Enter the below details and click 'Apply':

- o Name : Name of the Authentication Scheme
- o Authentication Level : 1
- o Challenge Method : BASIC
- o Challenge Redirect URL : /oam/server
- o Authentication Module : LDAPOverOUD
- o Refer the section 'Creating Authentication Module 2.6.2' of this document.
- o Challenge Parameters : ssoCookie=http
contextType=default
contextValue=/oam
challenge_url=/CredCollectServlet/BASIC

Form Style Authentication Scheme

Enter the below details and click 'Apply':

- Name : Name of the Authentication Scheme
 - Authentication Level : 2
 - Challenge Method : FORM
 - Challenge Redirect URL : /oam/server
 - Authentication Module : LDAPOverOUD
 - Challenge URL : /pages/login.jsp
 - Context Type : default
 - Context Value : /oam
 - Challenge Parameters : ssoCookie=http
10. We need to add the 'enforce-valid-basic-auth-credentials' tag to the config.xml file ,located under <weblogic deployment path>/user_projects/domains/<MyDomain>/config/. The tag must be inserted within the <security-configuration> tag as follows: [Just above </security-configuration> tag]
<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
11. Below JAVA_OPTION in setDomainEnv.sh of OAM_DOMAIN:
JAVA_OPTIONS="{ JAVA_OPTIONS} -
Dweblogic.configuration.schemaValidationEnabled=false"
export JAVA_OPTIONS
12. Add LOC_CODE=<FCUBS user home branch code> with PARAM_NAME=SSO_INSTALLED and PARAM_VALUE=Y in CSTM_BRANCH_LOC_PARAMS table.

2.7 Install and Configure Oracle HTTP Server 12c

2.7.1 Install Oracle HTTP Server

1. Launch a terminal window and enter the following command to install OHS:
cd /stage
chmod +x fmw_12.2.1.3.0_ohs_linux64.bin
./fmw_12.2.1.3.0_ohs_linux64.bin
2. Follow the table below to guide you through the installation screens:

Step	Window	Choices or Values
1.	Welcome	Click Next
2.	Auto Updates	Click Next
3.	Installation Location	Oracle Home: /u01/app/oracle/product/middleware/

4.	Installation Type	Collocated HTTP Server (Managed through WebLogic Server)
5.	Prerequisite Checks	Click Next
6.	JDK Selection	JDK Home: /u01/app/oracle/product/jdk
7.	Prerequisite Checks	Click Next
8.	Installation Summary	Click Install . The installation screen will appear*
9.	Installation Complete	Click Finish

2.7.2 Configure HTTP Server

1. Launch a terminal window as `oracle` and enter the following command to stop the WebLogic Admin Server:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
./stopWebLogic.sh
```
2. Run the following command to launch the Configuration Wizard:

```
cd /u01/app/oracle/product/middleware/oracle_common/common/bin
./config.sh
```
3. Follow the table below to guide you through the configuration screens:

Step	Window	Choices or Values
1.	Create Domain	Select Update an existing domain Domain Location: /u01/app/oracle/admin/domains/oam_domain
2.	Templates	Oracle HTTP Server (Collocated)
3.	Database Configuration Type	Get RCU Configuration Click Next
4.	Component Datasources	Click Next
5.	JDBC Component Schema Test	Click Next
6.	Advanced Configuration	System Components

7.	System Components	Click Add System Component: ohs1
8.	OHS Server	Click Next
9.	Machine	Click Next
10.	Assign System Components to Machines	Select ohs1 and oam_machine and click the arrow to move ohs1 under oam_machine
11.	Configuration Summary	Click Update
12.	Configuration Progress	Click Next
13.	End of Configuration	Click Finish

2.7.3 Start the Servers

1. Launch a terminal window and run the following command to start the WebLogic AdminServer. Enter `weblogic/Welcome1` as the username and password when prompted:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
./startWebLogic.sh
```

2. In another terminal window run the following command to stop and start Node Manager:

```
nohup ./startNodeManager.sh &
```

3. In the same terminal window run the following command to start Oracle HTTP Server. Enter `Welcome1` as the password when prompted:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
./startComponent.sh ohs1
```

4. Following to show after OHS successfully started-

```
Successfully Connected to Node Manager.
Starting server ohs1 ...
Successfully started server ohs1 ...
Successfully disconnected from Node Manager.
Exiting WebLogic Scripting Tool.
Done
```

5. Launch a browser and check the OHS is accessible by accessing the URL <http://oam.example.com:7777>

2.8 Creating OAM 12c Webgate

Follow the below steps to create a Webgate:

1. Launch a terminal window as oracle and enter the following command:

```
cd /u01/app/oracle/product/middleware/webgate/ohs/tools/deployWebGate
./deployWebGateInstance.sh -w \
/u01/app/oracle/admin/domains/oam_domain/config/fmwconfig/components/OHS/instance/ohs1 \
-oh /u01/app/oracle/product/middleware/
```

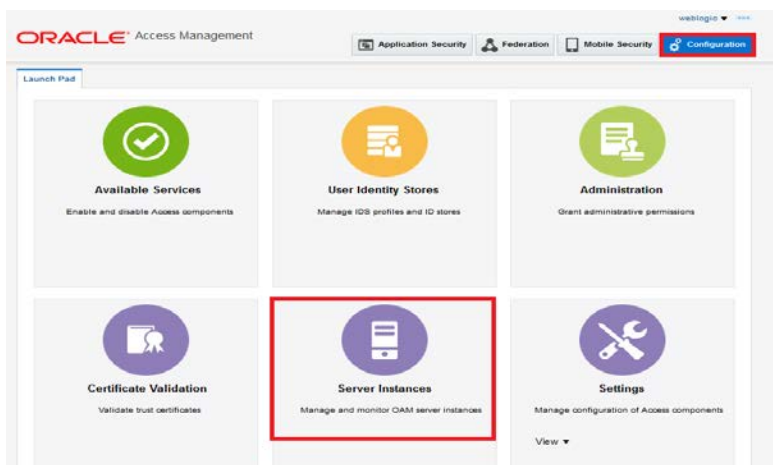
2. Check that a webgate directory and subdirectories were created:

```
ls -lart
/u01/app/oracle/admin/domains/oam_domain/config/fmwconfig/components/OHS/instance/ohs1/web
gate/
total 16
drwxr-x--- 7 oracle oinstall 4096 Aug 16 07:12 ..
drwxr-xr-x 4 oracle oinstall 4096 Aug 16 07:12 .
drwxr-xr-x 3 oracle oinstall 4096 Aug 16 07:12 tools
drwxr-xr-x 3 oracle oinstall 4096 Aug 16 07:12 config
```

3. Run the following command:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/u01/app/oracle/product/middleware/lib
cd /u01/app/oracle/product/middleware/webgate/ohs/tools/setup/InstallTools
./EditHttpConf -w
/u01/app/oracle/admin/domains/oam_domain/config/fmwconfig/components/OHS/instance/ohs1 \
-oh /u01/app/oracle/product/middleware/
```

4. Register the WebGate with OAM by click on 'Server Instances' under Configuration.



5. Click on 'Search'.

The screenshot shows the Oracle Access Management console. The 'Server Instances' tab is active. Under 'Search OAM Servers', there is a 'Search' section with a 'Name' input field. To the right of the input field are 'Search' and 'Reset' buttons. The 'Search' button is highlighted with a red box. Below the search section is a 'Search Results' table with columns 'Row' and 'Name'. The table is currently empty, showing 'No data to display'.

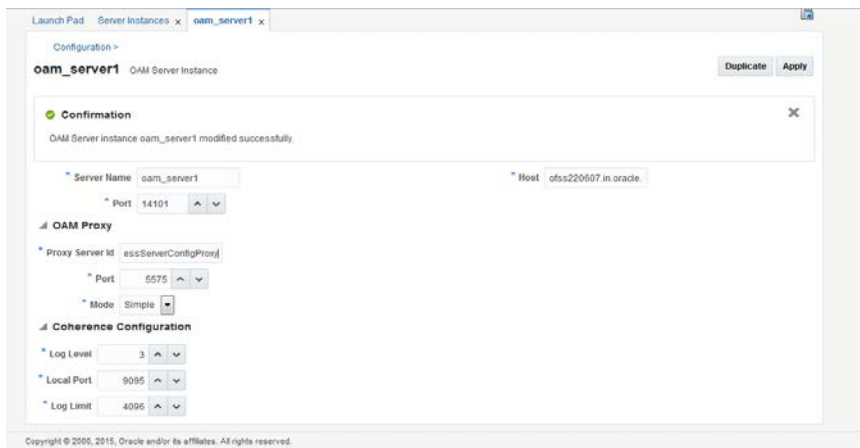
6. Edit oam_server1.

The screenshot shows the Oracle Access Management console. The 'Server Instances' tab is active. Under 'Search OAM Servers', the 'Search' section is empty. The 'Search Results' table now contains one entry: 'oam_server1'. This entry is highlighted with a red box. The table has columns 'Row' and 'Name'.

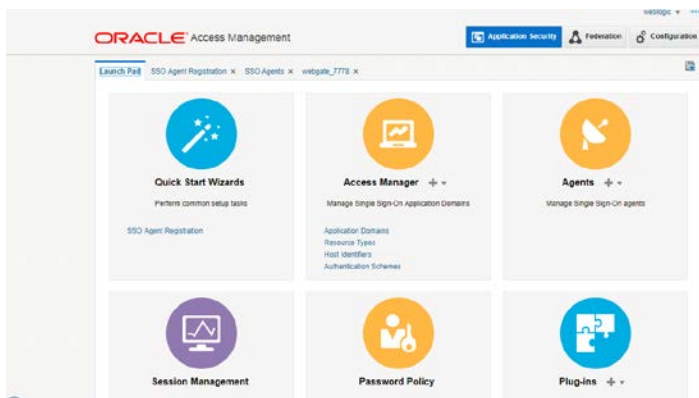
7. Modify the Mode from Open to Simple and click on 'Apply'.

The screenshot shows the Oracle Access Management console. The 'Server Instances' tab is active, and the 'oam_server1' instance is selected. The configuration page for 'oam_server1' is displayed. Under the 'Coherence' section, the 'Mode' is set to 'Simple'. The 'Simple' option is highlighted with a red box. The 'Apply' button is also highlighted with a red box.

The screenshot shows the Oracle Access Management console. The 'Server Instances' tab is active, and the 'oam_server1' instance is selected. The configuration page for 'oam_server1' is displayed. A 'Confirm Edit' dialog box is shown in the foreground, asking 'OAM Server instance oam_server1 might be in use. Are you sure you want to edit it?'. The 'Yes' button in the dialog is highlighted with a red box.



8. Click on SSO Agent Registration



9. Fill the value and click Finish—

SSO Agent Registration
Select the type of SSO Agent that you want to register and configure it.

Back Agent Type Configure Finish Cancel Next

Configure Webgate

Name
Description
Base URL
Access Client Password
Host Identifier
User Defined Parameters

Security ☒ Open
☐ Simple
☐ Cert

Virtual host ☐
Auto Create Policies ☒
IP Validation ☐

Resource Lists

Protected Resource List Add Delete

Relative URI

Public Resource List Add Delete

Relative URI
No data to display

Select **Agent Type**: Webgate and click **Next**.

On the **Configure WebGate** page enter details as follows, and then click **Finish**:

Name : Custom Webgate Name

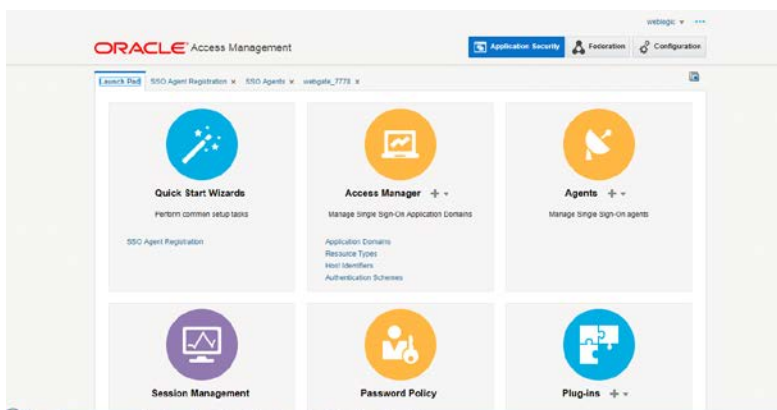
Base URL : The host and port of the computer on which the Web server for the Webgate is installed. For example, http://example_host:port or https://example_host:port. The port number is optional.

Security : Simple

Protected Resource List : for FCUBS : /FCJNeoWeb
For FCIS : /FCISNeoWeb

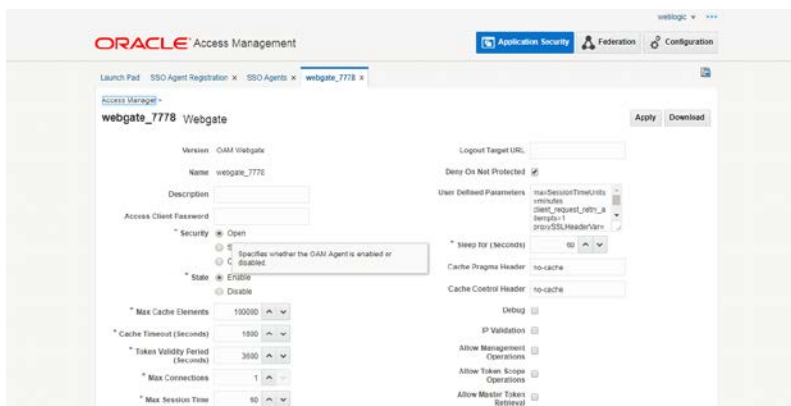
User Defined Parameters : filterOAMAuthnCookie=false

10. Click “Agent” in Application Security



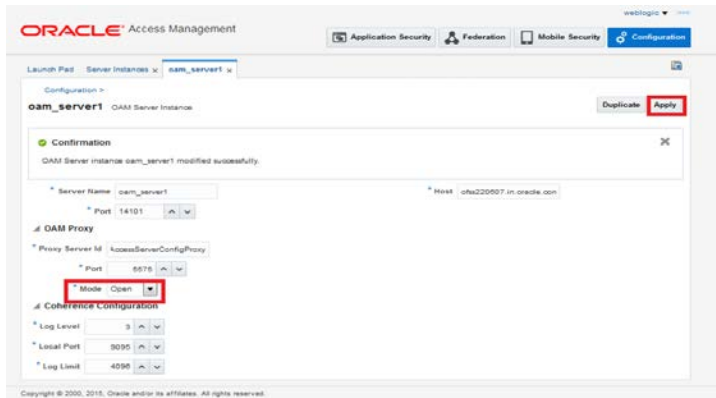
11. Click Search and open the Webgate Agent created in the above step.

Change the value in User Definer Parameters to below
proxySSLHeaderVar=nonssl



12. Click on ‘Apply’.

13. Change the value of Mode back to Open in oam_server1 on Server Instance and click ‘Apply’.



14. Click **Download** and save the webgate_7777.zip to /stage.

15. Copy the WebGate zip in the below directory and unzip-

/domains/OAM_domain/config/fmwconfig/components/OHS/ohs1/webgate/config

16. Modify the value in httpd.conf present in below location:

/domains/OAM_domain/config/fmwconfig/components/OHS/ohs1/

Add the below text at the end of the file

include "webgate.conf"

17. Restart the Servers

Launch a terminal window as oracle and run the commands below to stop all the servers.

Enter weblogic and Welcome1 for username and password if prompted:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
```

```
./stopComponent.sh ohs1
```

```
./stopNodeManager.sh
```

```
./stopManagedWebLogic.sh oam_policy_mgr1
```

```
./stopManagedWebLogic.sh oam_server1
```

```
./stopWebLogic.sh
```

Run the following commands launching new terminal windows as oracle to start the servers:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
```

```
./startWebLogic.sh
```

```
./startManagedWebLogic.sh oam_server1
```

```
./startManagedWebLogic.sh oam_policy_mgr1
```

```
./startNodeManager.sh
```

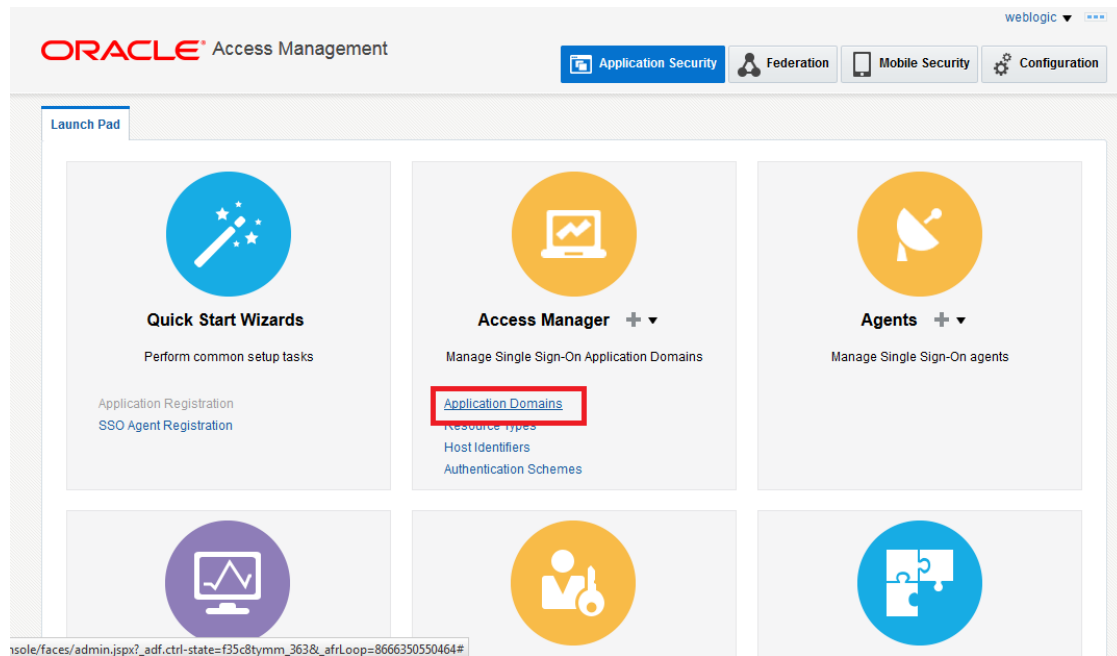
```
./startComponent.sh ohs1
```

2.8.1 Post OAM Webgate 12c Creation

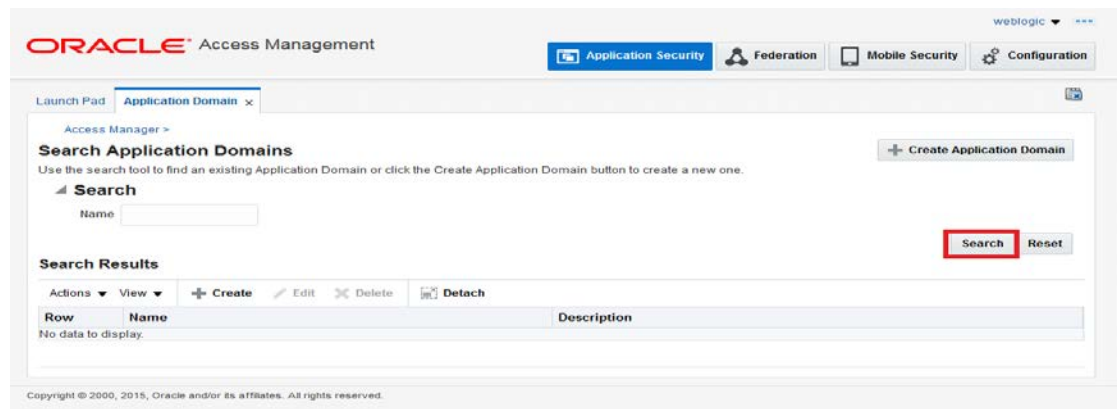
Follow the below steps to configure the webgate created.

2.8.1.1 Application Domains Changes

18. Click on 'Application Domains' in Access Manager under Application Security



19. Click on 'Search' to find the Webgate.



ORACLE Access Management

weblogic

Application Security Federation Mobile Security Configuration

Launch Pad Application Domain x

Access Manager >

Search Application Domains

Use the search tool to find an existing Application Domain or click the Create Application Domain button to create a new one.

Search

Name

Search Reset

Search Results

Actions View Create Edit Delete Detach

Row	Name	Description
1	FlexcubeWebgate	Application Domain created through Remote Registration
2	Fusion Apps Integration	Policy objects enabling integration with Oracle Fusion Applications
3	IAM Suite	Policy objects enabling OAM Agent to protect deployed IAM Suite applications

20. Click on 'Authentication Polices'.

ORACLE Access Management

weblogic

Application Security Federation Mobile Security Configuration

Launch Pad Application Domain x FlexcubeWebgate x

Access Manager >

FlexcubeWebgate Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Summary Resources **Authentication Policies** Authorization Policies Token Issuance Policies Administration

Apply

* Name FlexcubeWebgate

Description Application Domain created through Remote Registration

* Session Idle Timeout (minutes) 0

Allow OAuth Token ☐

Allow Session Impersonation ☐

Enable Policy Ordering ☐

21. Click on 'Protected Resource Policy'.

ORACLE Access Management

weblogic

Application Security Federation Mobile Security Configuration

Launch Pad Application Domain FlexcubeWebgate

Access Manager >

FlexcubeWebgate Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Summary Resources **Authentication Policies** Authorization Policies Token Issuance Policies Administration

Select an existing Authentication Policy from the list or click the Create Authentication Policy button to create a new one.

Actions View + Create Duplicate Edit Delete Detach

Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
2	Protected Resource Policy	Policy set during domain creation. Add resources to this policy to protect them.

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

22. Choose the Authentication Scheme created earlier in 'Creating Authentication Scheme'.

Launch Pad Application Domain FlexcubeWebgate FlexcubeWebgate : Protect...

Access Manager >

Protected Resource Policy Authentication Policy

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

Name Protected Resource Policy Success URL Failure URL

Description Policy set during domain creation. Add resources to this policy to protect them.

Select the challenge mechanism required to authenticate the user.

Authentication Scheme

- LDAPScheme
- AdaptiveAuthenticationScheme
- AnonymousScheme
- BasicFAScheme
- BasicScheme
- BasicSessionlessScheme
- ESSOProvAuthnScheme
- FAAdminLocalScheme
- FAAuthScheme
- FederationMTScheme
- FlexcubeBasicOAMScheme
- FlexcubeFormOAMScheme
- FlexcubeKBAOAMScheme
- WebAccessScheme
- LDAPNoPasswordValidationScheme
- LDAPScheme
- OAMAdvanced
- OAMBasic
- OAM10gScheme
- OAMAdminConsoleScheme

Resources

Resource To This Policy

Query String

Duplicate Apply

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

23. Click 'Responses' tab and click + Add button to Add 'DN' variable to the Response Header.

Protected Resource Policy Authentication Policy

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

* Name: Protected Resource Policy

Description: Policy set during domain creation. Add resources to this policy to protect them.

* Authentication Scheme: FlexcubeBasicOAMScheme

Success URL:

Failure URL:

Resources **Responses** Advanced Rules

— Identity Assertion

This will cause an assertion to be generated for the user, optionally containing any Asserted Attribute set below.

Responses **+ Add** Edit Delete

Name	Type	Value
This Policy does not have any Responses		

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

24. Enter the following values in the Add Response Window:

Type : Header

Name : DN

Value : \$user.attr.dn

Click on Add button

Add Response

* Type: Header

* Name: DN

* Value: \$user.attr.dn

Identity Assertion has not been enabled for this policy. Enable Identity Assertion in order

Add Cancel

25. Click on Apply to Save the Changes

Launch Pad Application Domain x FlexcubeWebgate x FlexcubeWebgate : Protect... x

Access Manager >

Protected Resource Policy

Authentication Policy

Authentication Policy defines the type of verification that must be performed to provide a sufficient level of trust for Access Manager to grant access to the user making the request. A single policy can be defined to protect one or more resources in the Application Domain.

[Duplicate](#) [Apply](#)

Confirmation

Authentication Policy, Protected Resource Policy, modified successfully

* Name: Protected Resource Policy

Description: Policy set during domain creation. Add resources to this policy to protect them.

* Authentication Scheme: FlexcubeBasicOAMScheme

Success URL:

Failure URL:

Resources Responses Advanced Rules

☐ Identity Assertion

This will cause an assertion to be generated for the user, optionally containing any Asserted Attribute set below.

Responses + Add Edit Delete

Name	Type	Value
DN	Header	Suser.attr.dn

26. Click on 'Authorization Policies' and then click on 'Protected Resource Policy'.

ORACLE Access Management

Application Security Federation Mobile Security Configuration

Launch Pad Application Domain x FlexcubeWebgate x

Access Manager >

FlexcubeWebgate

Application Domain

Application Domain provides a logical container for resources or sets of resources, and the associated policies that dictate who can access specific protected resources.

Summary Resources Authentication Policies **Authorization Policies** Token Issuance Policies Administration

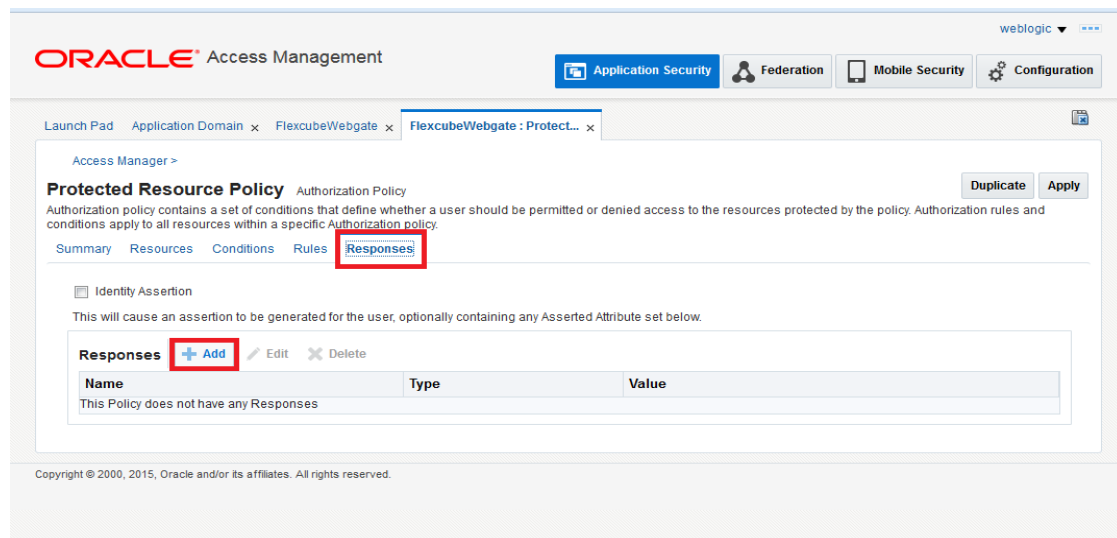
Select an existing Authorization Policy from the list or click the Create Authorization Policy button to create a new one.

Actions View + Create Duplicate Edit Delete Detach

Row	Name	Description
1	Public Resource Policy	Policy set during domain creation. Add resources to this policy to allow anyone access.
2	Protected Resource Policy	Policy set during domain creation. Add resources to this policy to protect them.

Copyright © 2000, 2015, Oracle and/or its affiliates. All rights reserved.

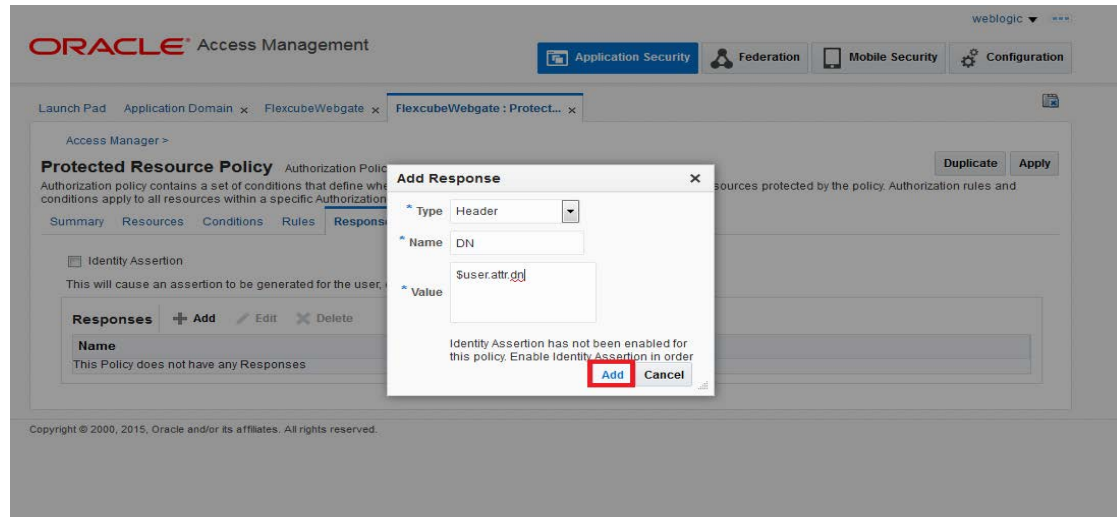
27. Click on 'Response' tab and click on [+ Add](#) button to Add 'DN' variable to the Response Header.



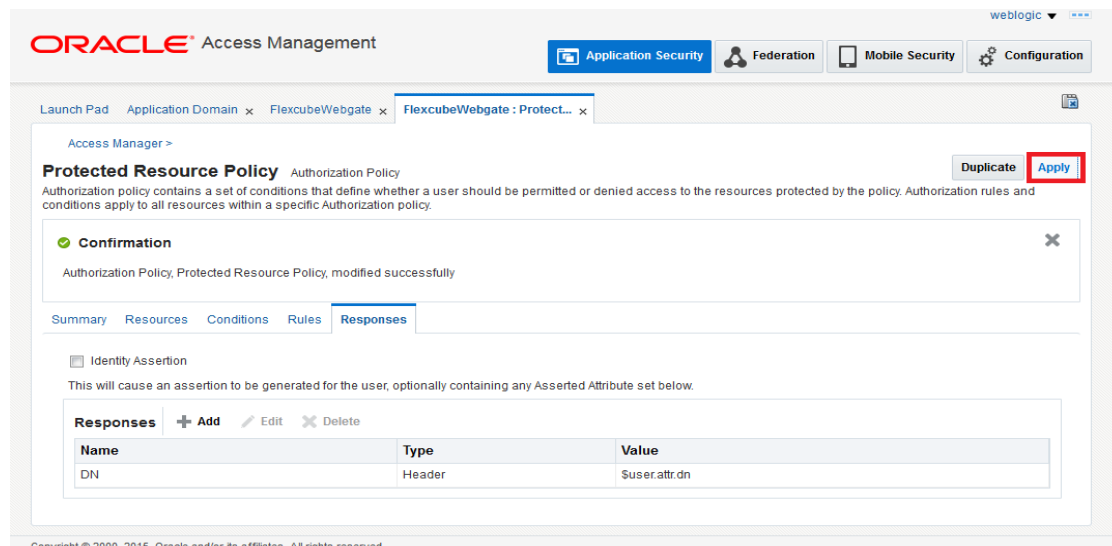
28. Enter the following values in the Add Response Window :

Type : Header
 Name : DN
 Value : \$user.attr.dn

Click on Add button



29. Click on 'Apply' to Save the changes.



2.8.1.2 Copying Generated Files and Artifacts to the Oracle HTTP Server WebGate Instance

Perform the following steps to copy the artifacts generated while creating the Oracle 12c Webgate to the Webgate installation directory:

- Navigate to <DOMAIN_HOME>/output/\$WebgateAgentName
- Select the following files
 - ObAccessClient.xml
 - password.xml
- cwallet.sso
 - cwallet.sso.lck

Copy the files to <ORACLE_MIDDLEWARE>/<ORACLE_WIBTIER_HOME> /instances/instance1/ config/OHS/ohs1/webgate/config/

/Middleware/OAM_Home/user_projects/domains/OAM_domain/config/fmwconfig/components/OHS/in stances/ohs1/webgate/config

- Select the remaining 2 files
 - aaa_key.pem
 - aaa_cert.pem
- Copy the files to <ORACLE_MIDDLEWARE>/<ORACLE_WIBTIER_HOME> /instances/instance1/ config/OHS/ohs1/webgate/config/simple

2.8.1.3 Configuring mod_wl_ohs for Oracle HTTP server Routing

To enable the Oracle HTTP Server instances to route to applications deployed on the Oracle Weblogic Server, add the directive shown below to the mod_wl_ohs.conf file available in <ORACLE_MIDDLEWARE> /<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1.

<Location /FCJNeoWeb>

SetHandler weblogic-handler

WebLogicHost ofss00002.in.oracle.com

WeblogicPort 7002

WLProxySSL OFF

SecureProxy OFF

WLSSLWallet

"<ORACLE_MIDDLEWARE>/<ORACLE_WEBTIER_HOME>/instances/instance1/config/OHS/ohs1/keystores/default"

</Location>

Note: In the above example, ofss00002.in.oracle.com is the server name where the Flexcube Application is deployed, 7002 is the SSL port and FCJNeoWeb is the context root of the FLEXCUBE application

2.8.1.4 Restart the Servers

1. Launch a terminal window as oracle and run the commands below to stop all the servers. Enter weblogic and Welcome1 for username and password if prompted:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
```

```
./stopComponent.sh ohs1
```

```
./stopNodeManager.sh
```

```
./stopManagedWebLogic.sh oam_policy_mgr1
```

```
./stopManagedWebLogic.sh oam_server1
```

```
./stopWebLogic.sh
```

2. Run the following commands launching new terminal windows as oracle to start the servers:

```
cd /u01/app/oracle/admin/domains/oam_domain/bin
```

```
./startWebLogic.sh
```

```
./startManagedWebLogic.sh oam_server1
```

```
./startManagedWebLogic.sh oam_policy_mgr1
```

```
./startNodeManager.sh
```

```
./startComponent.sh ohs1
```

2.8.1.5 Testing the FCUBS Application through WebGate

Close any open existing browsers and launch a new one. Access the OHS
URL: `http://oam.example.com:7777/FCJNeoWeb`



Oracle Access Manager Integration
[September] [2019]
Version 12.4.0.0.0

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
www.oracle.com/financialservices/

Copyright © [2007], [2019], Oracle and/or its affiliates. All rights reserved.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.